Computing, Performance and Communication Systems (2022)
Clausius Scientific Press, Canada
DOI: 10.23977/cpcs.2022.060106
ISSN 2371-8889 Vol. 6 Num. 1

Privacy Protection Data Aggregation Scheme with Batch Verification and Fault Tolerance in Smart Grid Communication

Baoyi Wang [a,*], Shengmei He[b] and Shaomin Zhang[c]

School of Control and Computer Engineering, North China Electric Power University, China
a. wangbaoyi@126.com, b. heshengmei0520@163.com, c. zhangshaomin@126.com
**corresponding author*

Keywords: smart grid, fault tolerance, anonymity, batch verification

Abstract: When collecting real-time fine-grained power consumption data in smart grid, it is very important to protect user privacy and data transmission, which has attracted more and more attention. However, smart devices such as smart meters may be maliciously damaged by users or stop running due to battery problems. In the smart grid, the problem of devices can not be ignored. As long as one device fails, it may not be decrypted, and even more serious, it will affect the power dispatching of the power system. In order to better protect the privacy of users and consider the fault-tolerant function, we propose a privacy protection data aggregation scheme with batch verification and fault tolerant in smart grid communication.

1. Introduction

When collecting real-time fine-grained power consumption data in smart grid, it is very important to protect user privacy and data transmission, which has attracted more and more attention. However, smart devices such as smart meters may be maliciously damaged by users or stop running due to battery problems[1]. In the smart grid, the problem of red devices can not be ignored. As long as one device fails, it may not be decrypted, and even more serious, it will affect the power dispatching of the power system. In order to better protect the privacy of users and consider the fault-tolerant function, we propose a privacy protection data aggregation scheme with batch verification and fault-tolerant capability in smart grid communication.In summary, the contribution of this paper is as follows: a privacy protection scheme of smart home electricity information based on plug-in electric vehicle is proposed in this paper, and gives a smart home electricity load model with electric vehicle energy storage. The multi-objective function of electricity cost and privacy protection reduces the user's electricity cost while ensuring user privacy.

In order to better protect the privacy of users and consider the fault-tolerant function, so that when a meter has a problem, it can find the problem meter and decrypt it. We propose a privacy

preserving data aggregation scheme with batch verification and fault tolerance in smart grid communication. In smart grid, the combination of encryption algorithm and data aggregation scheme has the following advantages [2].

1) It can protect the user's privacy and resist the attack of malicious users. Even if the user is not authorized to obtain the user's power consumption information, the user's privacy cannot be analyzed.

2) It can reduce communication overhead, data storage cost and improve the speed of data analysis.

The rest of this paper is organized as follows. In the second section, we introduce the related work. In the third section, we introduce our scheme. In the fourth section ,we summarize the paper.

2. Related work

If the SG infrastructure is not provided with appropriate security protection mechanism, the power system may be powered off due to security attack. The unavailability of electricity in modern cities will lead to the collapse of normal life. In terms of privacy, if customers' private data is obtained by malicious users, it will have a negative impact on their lives. In order to provide better security for smart grid infrastructure, a lot of research has been carried out.

Pailler encryption and BGN encryption are two typical homomorphic encryption. D. He [3] et al. Proposed a new P2DA scheme, which uses Boneh Goh Nissim public key cryptography technology to fight internal attackers, and uses Shamir's secret sharing to allow smart meters to negotiate aggregation parameters. However, when smart meters are widely used, it will cause slightly higher communication costs. Abdallah et al. [4] proposed using vector space structure to encrypt messages into noise lattice. Therefore, it mainly performs simple addition and multiplication operations in vector space to ensure the security of messages with low computational complexity. Zhou et al. [5] realized the combination of multi-level network and multi-dimensional data for the first time, which improved the practicability In this scheme, the combination of Paillier homomorphic encryption and blind factor is used to encrypt the user's multidimensional data, and the digital signature with efficient batch verification is used to reduce the number of bilinear pair operations required for the user's signature verification to a constant. Yang [6] considered data security and privacy protection. In terms of privacy protection, it considered the cost of differential privacy protection and power grid operation, as well as the design of demand forecasting framework through neural network technology. Guo [7] et al. proposed lightweight secure data aggregation of smart grid based on batch verification and applied the improved symmetric homomorphic encryption scheme. However, there is a defect in this paper, which can not resist collusion attack. Li et al. [8] set the sum of secret parameters of all devices to 0, but once one or more IOT devices fail, CC will not be able to decrypt the aggregated ciphertext. Guan et al. [9] proposed a device oriented anonymous privacy protection scheme, which uses pseudonym and pseudonym certificate and Paillier algorithm to ensure the privacy of data during data aggregation. However, this paper lacks application scenarios, and the generation and update of certificates are very time-consuming. Bae et al. [10] proposed a data communication scheme for AMI network, which can effectively aggregate the data into a single data packet and transmit it to the target domain through the concentrator, while preserving the user's privacy. However, it is necessary to further reduce the computational overhead of each encryption

algorithm to optimize the proposed scheme. Kan et al. [11] proposed a fault-tolerant fog enabled privacy protection secure data aggregation scheme. Data privacy is realized through Boneh Goh Nissan (BGN) encryption system. The case retains the data privacy of measurement data, ensures source authentication, supports fault tolerance, and prevents wrong data injection (FDI) attacks. Amin et al.[12] proposed a new homomorphic privacy protection protocol (called NHP3), which has fault tolerance and supports multi category aggregation, but it is not used for user authentication. Chen et al.[13] proposed the research on data encryption and signature in smart grid, and the pseudonym generation proposed therein is worthy of further study.

3. Scheme design

Our system includes four entities: KGC, SM, GW and CC. As shown in Figure 1 below, they are smart meter (SM), gateway (GW), power control center (CC) and key generation center (KGC). In this scheme, the residential area is taken as the unit. Residential user is equipped with smart meters and various smart appliances. Smart meters can electronically record real-time fine-grained power consumption data and report it to CC through GW.

Smart meter (SM) is a trusted meter. It is responsible for collecting the power consumption data of various appliances in each family, encrypting it and sending it to the gateway.

Gateway (GW) is a powerful entity connecting CC and residential users, that is, it helps CC collect near real-time usage data of residential users. GW manages smart meters in corresponding areas, authenticates the legitimacy of data transmitted by smart meters, and aggregates encrypted data. After that, the GW sends the aggregated and signed power consumption data to CC through the secure channel.

The function of the key generation center (KGC) can be borne by trusted third parties such as banks and Alipay. KGC is responsible for generating some private keys and public keys for SM and CC, and generating pseudo identities for users. KGC only retains some public and private keys, as well as the user's pseudo identity. Generally, KGC will go offline after initializing the system.

The power control center (CC) is responsible for decrypting and analyzing the collected aggregated data. Then CC uses the obtained data for real-time dynamic pricing and billing.

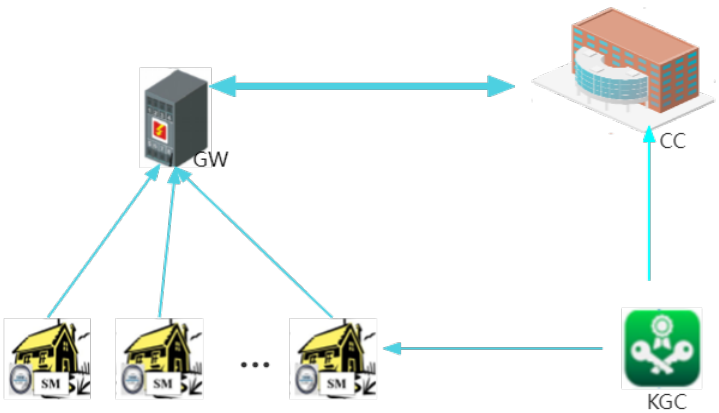

Figure 1: System model architecture diagram.

The proposed scheme is divided into four tasks: key generation, SM encryption and signature generation, signature verification and fault-tolerant aggregation of GW, and decryption of aggregated data of CC.

3.1. Key generation

KGC needs to generate the key of BGN encryption system and the secret parameters of SM and CC for fault-tolerant decryption. The KGC randomly selects two large primes $p_1 = 2p + 1$ and $q_1 = 2q + 1$, where p and q are also two large primes, so that $n = p_1 q_1$,$G, G_1$are two n order multiplication groups with bilinear pairings, $e: (G * G) \to G_1$.. Select two random generators g, u from group G and set $\eta = u^{q_2} \bmod n$. Public and private keys are generated as $pk = (n, G, G_1, e, g, \eta)$ and $sk = p_1$.Then,KGC generates the user's pseudo identity $PID_i = H(ID_i||t)$ according to the user's real identity ID_i. Where $H(\cdot)$ is the hash function, t is the timestamp, and KGC obtains the signature secret key of $User_i$ .After KGC determines the parameter $s \in Z_p^*$, $y = g^s$ is used as the public key. Then find the following formulas in turn (1)-(2).

$$pid_i = H(PID_i, ID_i) \quad (1)$$

$$S_i = pid_{i,0}^s \quad (2)$$

Where S_i is the user's signature secret key. Then KGC sends $(PID_i, S_i)$to $User_i$.In addition, according to Lagrange's formula, we can have $G(x) = \sum_{j=1}^{n} \prod_{i=1, i\neq j}^{n} \frac{x_i - x}{x_i - x_j}$, $\beta_{x_i} = \prod_{j\neq i}^{n} \frac{x_j}{x_i - x_j}$ .Then, we can easily calculate as follows:$\sum_{i=1}^{n} G(x_i)\, \beta_{x_i} = 0$. KGC uses the above formula to obtain n secret private keys $(x_i, G(x_i), \beta_{x_i})$ and distribute them to the corresponding smart meter equipment, n represents the number of users, where x_i is the random number representing the SM_i serial number.

3.2. SM encryption and signature generation

This task is responsible for encryption and signature generation. Each SM_i encrypts the collected power consumption data $m_i$of each user through the secret key $(S_i, x_i, G(x_i), \beta_{x_i}, pk, sk, PID_i)$and digital signature σ_i .Encryption and digital signature operations are performed by equations (3)-(4). Then submit ciphertext c_i and σ_i to GW.

$$c_i = E(m_i) = g^{m_i} \eta^{rG(x_i)\beta_{x_i}} \quad (3)$$

The $User_i$ signs with the signature secret key, where $h_i = H(m_i, PID_i, t)$. As in formula

$$\sigma_i = S_i^{h_i} \quad (4)$$

Where $H(\cdot)$ is a hash function , m_i is the message sent by the user, and t is the timestamp of a specific time slot. The user sends$(c_i, \sigma_i, PID_i, x_i, t)$ to GW for verification.

3.3. Signature verification and fault-tolerant aggregation of GW

In this task, GW maintains a multi-column list of information. The list has three columns $(x_i, flag, c_i)$. At the beginning of each round of data collection activity, the flag column value for each SM is set to 0. Once data is received from a particular SM, the GW verifies its signature σ_i.If the signature is verified, the GW will update the flag value to 1 for the SM. The GW also stores a copy of the metering data in a buffer for SM. GW summarizes the ciphertext received from the connected SM within its jurisdiction. GW verifies the number of all SM in its jurisdiction according to the flag value in the information list. If an instrument in the sg network fails, the SM will adjust its missing reading based on the last successfully received reading of the stored value in the buffer. In addition, GW interacts with KGC, and KGC obtains the blind factor$(x_i, G(x_i), \beta_{x_i})$ of the failed smart meter according to x_i the collected list information. Aggregation activities are calculated by formulas (5),(6) and (7). The aggregated data is first verified by formula (6) and (7) of the aggregation formula, and then sent to the GW through formula (6). If there are no failed instruments, use equation (6), otherwise use equation (7). It is assumed that at least one success value of each SM configured in the sg network is stored in the buffer.

First, GW collects the signatures sent by the user for batch verification, as in formula (5).

$$\sigma = \prod_{i=1}^{n} \sigma_i \tag{5}$$

If $e(\sigma, g) = e(\prod_{i=1}^{n} pid_i^{h_i}, y)$ is established, it indicates that the visa is successful.

$$C = \prod_{i=1}^{n} c_i \tag{6}$$

$$C = \prod_{i=1}^{w} c_i + \prod_{i=1}^{n-w} buf(c_i) \tag{7}$$

3.4. Decryption of CC

In this task, CC summarizes the data sent by GW. The decryption activity is performed through the equation. (8)(9)(10).

$$C = g^{\Sigma_i^n m_i} \eta^{r \Sigma_i^n G(x_i) \beta_{x_i}} \tag{8}$$

CC calculation

$$C\eta^{-r} = g^{\Sigma_i^n m_i} \tag{9}$$

CC calculates the discrete logarithm $g^{\Sigma_i^n m_i}$ and uses Pollard's lambda method to obtain M_{sum}, as shown in the equation.

$$M_{sum} = \sum_{i}^{n} m_i \tag{10}$$

4. Conclusion

This paper proposes a privacy protection data aggregation scheme with batch verification and fault tolerance in smart grid communication. The main contribution of this scheme is to anonymize user identity. It supports batch authentication and is fault-tolerant. It resists curiosity GW and CC, and does not allow them to infer detailed user data, so as to protect user privacy. Secondly, because the blind factor is added in this paper, even if the malicious user monitors the power consumption data through the channel, the user's privacy cannot be obtained. Compared with other Paillier homomorphic encryption schemes, it is lightweight and especially suitable for smart meters with scarce computing resources. As a future work, we hope to reduce the computational and communication overhead in the whole process by using novel encryption methods.

References

[1] P. Gope and B. Sikdar.Privacy-aware authenticated key agreement scheme for secure smart grid communication[J]. IEEE Trans. Smart Grid,VOL. 10, NO. 4, Pages:3953-3962, Jul. 2019.

[2] X. Wang .Research on fault tolerant data aggregation protocol [D]. Guilin University of Electronic Science and technology, 2021.

[3] D. He, N. Kumar, S. Zeadally, A. Vinel and L. T. Yang.Efficient and Privacy-Preserving Data Aggregation Scheme for Smart Grid Against Internal Adversaries[J]. IEEE Transactions on Smart Grid, VOL. 8, NO. 5, Pages:2411-2419, Sept. 2017.

[4] Abdallah, A., Shen, X.S .A Lightweight Lattice-Based Homomorphic Privacy-Preserving Data Aggregation Scheme for Smart Grid[J]. IEEE Transactions on Smart Grid,2016.

[5] H. Zhou, J. Chen, Y. Zhang, L. Dang.A Multidimensional Data Aggregation Scheme in Multilevel Network in smart grid[J]. Journal of cryptography, VOL.4,NO.2,Pages:114-132,2017.

[6] Z. Yang .Research on user data security and privacy protection in smart grid [D]. Zhejiang University, 2017.

[7] Guo, C., Jiang, X., Choo, K.-K.R., Tang, X., Zhang, Lightweight privacy preserving data aggregation with batch verification for smart grid[J]. Future Generation Computer Systems 112, Pages:512-523,2020..

[8] Li, X., Liu, S., Wu, F., Kumari, S., Rodrigues, J.J.P .C. Privacy Preserving Data Aggregation Scheme for Mobile Edge Computing Assisted IoT Applications[J]. IEEE Internet Things , VOL .6,Pages: 4755-4763,2019.

[9] Guan, Z., Si, G., 2017. Achieving privacy-preserving big data aggregation with fault tolerance in smart grid[J]. Digital Communications and Networks,VOL. 3, Pages:242-249,2017.

[10] Bae, M., Kim, K., Kim, H. Preserving privacy and efficiency in data communication and aggregation for AMI network[J]. Journal of Network and Computer Applications,VOL. 59, Pages:333-344, 2015.

[11] Khan, H.M., Khan, A., Jabeen, F., Rahman, A.U. Privacypreserving data aggregation with fault tolerance in fog-enabled smart grids[J]. Sustainable Cities and Society ,VOL.64, 2020.

[12] Mohammadali, A., Haghighi, M.S.A Privacy-Preserving Homomorphic Scheme With Multiple Dimensions and Fault Tolerance for Metering Data Aggregation in Smart Grid[J]. IEEE Transactions on Smart Grid ,VOL.12, Pages:5212-5220, 2021.

[13] S. Chen, J. Zhang, Z. Ni, J. Li, H. Lin, J. Li, Research on data encryption and signature in smart grid [J] Microcomputer application, VOL.36 ,NO.09,Pages: 83-85 + 100, 2020.